VIRGINIA JOURNAL OF LAW & TECHNOLOGY

WINTER 2004 UNIVERSITY OF VIRGINIA VOL. 9, NO. 3

The Wiretap Act and Web Monitoring:
A Breakthrough for Privacy Rights?

YONATAN LUPU†

ABSTRACT

As Web sites have sought to distinguish themselves from their competitors in recent years, many Web site operators have turned to Web monitoring devices, such as cookies, as a means of customizing the sites to the individual user. Third-party businesses are increasingly performing this type of monitoring as a service to Web sites, by placing their own code into their client site's code, collecting the data using their own servers, and then processing the data into aggregate statistics or even personalized profiles of visitors.

The benefits afforded by this technology, however, are tempered by its capacity to capture – intentionally or unintentionally – personal information without notifying the average user. To protect their online privacy, individuals have relied on the Electronic Communications Privacy Act (ECPA), which allows for a private right of action against certain interceptions of electronic communications. However, the ECPA provides an exception for the interception of communications when a party to the communication has consented to the interception. Consequently, privacy challenges to the use of cookies routinely failed when the Web site operator had consented to the electronic interception of the cookie by third-party businesses. The First Circuit's decision in *In re Pharmatrak*, however, revived this argument and seemed to indicate an increased willingness to limit the use of Web monitoring devices. Nonetheless, as this article concludes, this decision is limited to its relatively unusual facts and is therefore likely to do little to affect all but the most malicious and disreputable Web monitors.

† Associate, Shaw Pittman LLP, Washington, D.C. Thanks to Jeremy Schropp for his assistance in the preparation of this article.

TABLE OF CONTENTS

I. INTRODUCTION

¶ 1 With the number of Internet users rapidly approaching 700 million worldwide,[1] it is easy to recognize why businesses, politicians, musicians, sports teams, government agencies, and individuals are willing to invest increasing amounts of time and money to create flashy Web sites designed to lure a greater share of the electronic audience. Competition is fierce on the Internet, and in order to boost their visitor numbers, site operators must attempt to distinguish themselves. Increasingly, they have sought innovative ways to design sites that are more user-friendly, cater to a particular demographic, and are customized to individual visitors.

¶ 2 As site operators have learned, these goals can be advanced significantly through the use of codes embedded in a Web site that allow the operator to gather a wide variety of information from Internet users. Among the most popular of these Web-monitoring devices are "cookies." When a user contacts a particular Web site, its cookie is sent to his or her hard drive. The cookie then begins collecting data about the user, including the date and time of the visit, the specific pages within a site the user accessed, and often the information the user gave when filling out online forms. The next time the user accesses the Web site, the stored information is retrieved from the user's computer and delivered back to the site's server. The site operator is thus able to retrieve information ranging from the number of first-time versus repeat visits to the types of pages accessed by

1. While calculating the exact number of Internet users is an imprecise task, the United Nations' projected forecast for the end of 2002 was 655 million users worldwide. *E-Commerce and Development Report 2002*, United Nations Conference on Trade and Development, at xix (2002), *available at* http://r0.unctad.org/ecommerce/docs/edr02_en/ecdr02.pdf (last visited Jan. 17, 2003).

individual users. Cookies and other Web-monitoring devices, although virtually undetectable to Web surfers, can therefore convey valuable and often sensitive information about them. This information is often used to provide greater convenience to the user. For example, a cookie can remember preferences or login information so that such information does not have to be re-entered each time the user visits the site.[2]

¶3 As part of the general increase in the use of Web-monitoring tools over the last few years, third-party businesses are increasingly performing this type of monitoring as a service to Web sites. These companies place their own code into their client site's code, collect the data using their own servers, and then process the data into aggregate statistics or even personalized profiles of visitors. Some service providers even promise to provide an analysis, based on data obtained from cookies, as to how a client site ranks with respect to its competitors. A 1998 Federal Trade Commission (FTC) survey showed that 85% of the 1400 Web sites it surveyed collected personal data on their visitors.[3] Another FTC study of the busiest Web sites found that roughly 78% allowed third parties to place cookies on their sites.[4]

¶4 The benefits afforded by this technology, however, are tempered by its capacity – intentionally or unintentionally – to capture personal information without notifying the average user. Web site operators justify the use of monitoring devices as a means of learning more about their visitor, knowledge they use to tailor their Web sites and

---

2. *See* Marshall Brain, *How Internet Cookies Work*, *at* http://computer.howstuffworks.com/cookie.htm (last visited Feb. 19, 2004); Viktor Mayer-Schönberger, *The Cookie Concept*, *at* http://www.cookiecentral.com/content.phtml?area=2&id=1 (last visited Feb. 19, 2004); Susannah Fox, *Trust and Privacy Online: Why Americans Want to Rewrite the Rules*, The Pew Internet & Am. Life Project, Aug. 20, 2000, *at* http://www.pewinternet.org/reports/toc.asp?report=19 (last visited Feb. 19, 2004). Web-monitoring devices generally operate in one of three ways: "get," "post," or "GIF" submissions. When the get method is used, information entered by the user is submitted to the recipient site as part of its URL. This results in the information being directly displayed in the browser's address bar. For example, a user inputting the terms "Cornell" "law" and "school" into a site using the get method would end up with a URL of "http://search.yahoo.com/bin/search?p=cornell+law+school." The post method, also known as the "put" method, does not incorporate information given by users into the URL. *See In re* Pharmatrak, Inc., Privacy Litig., 220 F. Supp. 2d 4, 8-9 (D. Mass. 2002) [hereinafter *Pharmatrak I*]; *'Tis Better to PUT than to GET, but it's the Contractual Thought that Counts* (May, 14, 2003), *at* http://www.ibusinesslaw.info./index.php?p=16&more=1 (last visited Feb. 19, 2004*). See also In re* DoubleClick, Inc., Privacy Litig., 154 F. Supp. 2d 497, 504 (S.D.N.Y. 2001); Janlori Goldman, Zoe Hudson & Richard M. Smith, California HealthCare Foundation, *Privacy: Report on the Privacy Policies and Practices of Health Web Sites* (2000), *at* http://www.informatics-review.com/thoughts/policy.html (last visited Feb. 19, 2004). The GIF (Graphic Interchange Format) method is also known as a Web bug, clear GIF, invisible GIF and beacon GIF. These are "invisible" because they are typically only 1 square pixel in size. When a user downloads a Web site containing a clear GIF, the website causes the user's computer to transmit certain information to the site's server or to a third party's server. Clear GIFs can transmit a user's IP address, the URL of the website that contained the GIF, the time of the visit, and previously stored cookie information. *See generally* Richard M. Smith, *The Web Bug FAQ* (Nov. 11, 1999), *at* http://www.eff.org/Privacy/Marketing/web_bug.html (last visited Feb. 19, 2004).

3. Federal Trade Commission, *Privacy Online: A Report to Congress*, at ii-iii (1998), *at* http://www.ftc.gov/reports/privacy3/priv-23a.pdf (last visited Feb. 19, 2004).

4. Federal Trade Commission, *Online Profiling: A Report to Congress* 11 (2000), *at* http://www.ftc.gov/os/2000/06/onlineprofilingreportjune2000.pdf (last visited Feb. 19, 2004).

maximize profitability. Cookies allow site operators to adjust to their visitors while also providing personalized touches. For example, cookies allow a Web site to provide easier access to the pages users visit most often. Cookies and other Web-monitoring tools are capable of storing everything from e-mail addresses to social security numbers to medical information – all without the user ever knowing this information has been collected or where it is headed. Nonetheless, the thought that their personal information may be floating around on the Internet, which can jeopardize their privacy and lead to an increase in SPAM e-mail, is understandably troubling to many individuals. Even in cases where a user intends to submit personal and identifying information to a site, he or she may be completely unaware that a third party is intercepting the transmission and delivering it to others as a service. For others, knowing that the communications they transmit via electronic medium may be compromised is a deterrent to utilizing online resources altogether.[5] Facing such uncertainty, individuals may be reluctant to, for example, search online for valuable information about a medical condition or may avoid engaging in electronic commerce.

¶ 5 To protect their online privacy, individuals have historically relied on common law privacy principles and various pieces of non-comprehensive privacy-related legislation. One statute often cited by those challenging Web monitoring is section 2511 of the Wiretap Act, [6] amended in 1986 by the Electronic Communications Privacy Act (ECPA).[7] As amended, section 2511 allows for a private right of action against certain interceptions of electronic communications.[8] Unfortunately for online privacy advocates, both statutes were drafted before the rise of the public use of the Internet and do not adequately address the interception of online information by Web monitors.[9] As a result, in recent years plaintiffs have been unsuccessful in a series of high-profile cases challenging the use of Web-monitoring tools under section 2511.[10] Last year, however, in *In re Pharmatrak* (*Pharmatrak II*), the First Circuit became the first court to allow a

---

5. *See, e.g.*, Nancy Lazar, *Consumers Online: Your Right to Privacy in Cyberspace*, 10 LOY. CONSUMER L. REV. 117, 117 (1998) (citing a poll that found that 78% of Americans would use the Internet more if given assurances that their personal information would be protected); Steve Lohr, *Survey Shows Few Trust Promises on Online Privacy*, N.Y. TIMES, Apr. 17, 2000, at C4 (citing a study by Odyssey, a market research firm, that found that 82% percent of Internet users agreed that the government should regulate online companies' use of personal information). *See also* S. REP. NO. 99-541, at 5 (1986) (noting that a lack of adequate protection "may unnecessarily discourage potential customers from using innovative communications systems").

6. Omnibus Crime Control and Safe Streets Act of 1968, Pub. L. No. 90-351, 82 Stat. 213 (1968) [hereinafter Wiretap Act].

7. 18 U.S.C. § 2510, *et seq.* (2000).

8. 18 U.S.C. § 2511(2)(a)(ii).

9. The Internet was created in 1969 as a project of several defense contractors, university laboratories, and the U.S. military. Even by the end of the 1980s, however, it was still used almost exclusively by the research, education, and government communities rather than general public. The explosion in the public and commercial use of the Internet came in the 1990s, following the creation of the World Wide Web and Web-browsing software. *See generally* ACLU v. Reno, 929 F. Supp. 824, 830-49 (E.D. Pa. 1996).

10. *See* Part II.B, *infra*; *In re* DoubleClick, Inc., Privacy Litig., 154 F. Supp. 2d 497 (S.D.N.Y. 2001); *In re* Intuit, 138 F. Supp. 2d 1272 (C.D. Cal. 2001); *In re* Toys R Us, Inc., Privacy Litig., 2001 U.S. Dist. Lexis 16947 (N.D. Cal.); Chance v. Avenue A., Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001).

claim under section 2511 against a Web site operator for the use of such tools.[11] In *Pharmatrak II*, the court reinstated a class action filed by users who claimed that Pharmatrak, a company that tracks information on its clients' Web sites, had improperly intercepted their personal information. The First Circuit reversed a district court finding (*Pharmatrak I*) that Pharmatrak's actions fell within the consent exception to the Wiretap Act and were therefore permissible.[12] The First Circuit's reversal demonstrates a general recognition by courts and legislatures that the protection of online privacy has become a major concern. At first look the decision seems to be a turning point in the fight by privacy advocates against the widespread practice of "Web-snooping," reversing the course taken by the cases that preceded it. In fact, when the decision was handed down analysts speculated that it could have serious implications for the use of cookies and other Web-monitoring devices.[13]

¶ 6 This article argues, however, that while *Pharmatrak II* shows that the ECPA amendments to the Wiretap Act impose certain limited restrictions on Web monitoring, the decision is so confined by its facts that it is unlikely to have significant long-term effects on the use of these tools or on the privacy of Internet users. Part II of this article begins by examining the scope of the Wiretap Act, the ECPA's protections and the exceptions to those protections, and the string of pre-*Pharmatrak II* decisions holding that section 2511 could not be used to stop Web monitoring. Part III then discusses the facts of the *Pharmatrak* cases, the district court decision, and the reasons for the First Circuit's reversal. Finally, Part IV analyzes the implications of the *Pharmatrak II* decision, including the loopholes it leaves open and the long-term impact it will have on users, site owners, and service providers such as Pharmatrak.

II. SECTION 2511 OF THE WIRETAP ACT

A. History and Purpose of the Wiretap Act and ECPA Amendments

¶ 7 Despite continuous calls for a definitive legislative stance on the protection of online privacy rights, Congress has not enacted a comprehensive statute. As a result, challenges to Web-monitoring devices such as cookies have often relied on broad privacy-related statutes such as the Wiretap Act and the ECPA. The Wiretap Act was enacted in 1968 in response to the Supreme Court's extension of Fourth Amendment protections to oral communications, including those by telephone, which were becoming increasingly easy to intercept.[14] The Wiretap Act made it illegal to intercept any wire or

11. *In re* Pharmatrak, Inc., Privacy Litig., 329 F.3d 9 (1st Cir. 2003) [hereinafter *Pharmatrak II*].

12. *Pharmatrak I*, 220 F. Supp. 2d 4 (D. Mass. 2002).

13. *See, e.g.*, Ben Worthen, *Court Opinion Raises Questions About Honeypots*, CIO MAGAZINE, July 15, 2003, *available at* http://www.cio.com/archive/071503/tl_washington.html (last visited Feb. 19, 2004); Leighton P. Roper III, *Case Study: Pharmatrak, Internet Cookies and Privacy*, *at* http://www.wcsr.com/CM/News Bites/NewsBites1686.asp (last visited Feb. 19, 2004).

14. *See* S. REP. NO. 99-541, at 2. The introduction of the bill closely followed Supreme Court decisions in *Berger v. New York*, 388 U.S. 41 (1967) (extending Fourth Amendment protection to electronic interception of oral communication) and *Katz v. United States*, 389 U.S. 347 (1967) (finding the Fourth Amendment applicable to telephone conversations).

oral communication except for certain specific exceptions, such as interception by law enforcement officials. The act, however, only protected those communications that could be "overheard and understood by the human ear."[15] The statute thus seemed inapplicable to much of the rapidly developing technology emerging in the mid-1980s.[16] Although data sent between computers via phone lines or cables may arguably constitute "wire communications," such transmission cannot be "understood by the human ears."[17] Accordingly, courts were reluctant to draw electronic communications into the restrictive definitions of the Wiretap Act.[18]

¶ 8 In 1986 Congress amended the Wiretap Act, seeking to bring under it the latest in electronic communication technology. Congress had concluded that advances in technology such as the Internet were being used "in lieu of, or side-by-side with" traditional mail and phone services.[19] The Senate report on the bill hinted at some of the dangers that could be generated by these advancements in computer-based data transmission. Specifically, it noted the creation of computerized record-keeping, which allowed for the storage of large databases of private information: "For the person or business whose records are involved, the privacy and proprietary interest in that information should not change. Nevertheless, because it is subject to control by a third-party computer operator, the information may be subject to no constitutional privacy protection."[20]

¶ 9 While the Senate report alluded to the potential of technology to continue its progression, Congress could not have foreseen the leaps in transmission speeds that would make electronic communications increasingly susceptible to interception.[21] As with the Wiretap Act, Congress seemed particularly focused on the threat posed by police surveillance and intended to update the statute to specify permissible uses of new

---

15. *See* S. REP. NO. 99-541, at 2 (citing United States v. New York Tel. Co., 434 U.S. 159, 167 (1977)).

16. By 1986, e-mail was beginning to emerge, as were cellular and cordless phones, pagers, electronic bulletin boards, and early forms of "computer-to-computer" transfers of data such as financial and medical records. *See* S. REP. NO. 99-541, at 2-3, 8-11.

17. Transmission of data across telephone lines requires a modem to convert digital signals to analog signals. The modem on the receiving end must then convert the signal back to digital. To the human ear, the signals being transferred across the telephone lines sound only like a series of beeps, tones, and static. *See* Ruel Torres Hernandez, *ECPA and Online Computer Privacy*, 41 FED. COMM. L.J. 17, 28 & n.36 (1988).

18. *See, e.g.*, United States v. Davey, 426 F.2d 842 (2dCir. 1970) (allowing an IRS-issued summons requiring a consumer credit organization to produce electronically stored individual credit reports).

19. S. REP. NO. 99-541, at 5.

20. *Id.* at 3.

21. In 1986, electronic data transmission was done almost exclusively via dial-up services, using modems with transmission speeds well below the maximum telephone line capacity of 56 kbps (kilobits per second). Even at that maximum rate, it would take several minutes to download a 1-megabyte file (such as a high-resolution graphic). By contrast, today's Internet users can connect via broadband connections such as cable modems. It can take as little as one second to download the same graphic file using a cable modem. *See generally*, National Cable Television Association and Tech Corps, *Surfing the Internet at Lightning Speed*, *at* http://www.yvn.com/Webteacher/cable/modemrev.html (last visited Feb. 19, 2004).

technology by law enforcement.[22] The words "Internet," "World Wide Web," and "e-commerce" appear in neither the ECPA nor its legislative history. When drafting the ECPA, Congress could not have contemplated that companies would be formed with the purposes of designing monitoring technology, seizing information from other users, bundling that information into aggregate statistics, and selling these to their clients. Thus, the ECPA did not directly address the complexity of today's communications infrastructure or the ease with which digital personal information can be intercepted.

¶ 10 Due to its use of a broad definition of "electronic communication," however, the ECPA can be interpreted to apply to the most advanced online transaction. The statute provides that "any person who — (a) intentionally intercepts, endeavors to intercept, or procures any other person to intercept or endeavor to intercept, any wire, oral, or electronic communication … shall be punished … or shall be subject to suit."[23] The ECPA amendments to the Wiretap Act added "electronic communications" to the list of protected content under section 2511 and defined this term as "any transfer of signs, signals, writing, images, sounds, data, or intelligence of any nature transmitted in whole or in part by a wire, radio, electromagnetic, photoelectronic, or photooptical system that affects interstate or foreign commerce …."[24] Thus in *Pharmatrak II*, the First Circuit affirmed earlier decisions holding that this additional language was sufficient to encompass the typical communications sent via the Internet, including the "[t]ransmission of completed online forms."[25]

¶ 11 Several exceptions to the general prohibitions were incorporated into the Wiretap Act and preserved in the ECPA amendments. These include rights for law enforcement officers and employees of electronic communications providers to intercept certain communications.[26] The most important exception (the "consent exception"), however, in the context of Web monitoring is the exception for:

> [A] person not acting under color of law to intercept a wire, oral, or electronic communication where such person is a party to the communication or one of the parties to the communication has given prior consent to such interception unless such communication is intercepted for the purpose of committing any criminal or tortious act.[27]

Largely because of this exception, section 2511 provides easily applicable loopholes that

22. The Senate report begins with Justice Brandeis' famous quote from *Olmstead v. United States*, 277 U.S. 438, 474 (1928): "Ways may some day be developed by which the Government, without removing papers from secret drawers, can reproduce them in court, and by which it will be enabled to expose to a jury the most intimate occurrences of the home. … Can it be that the Constitution affords no protection against such invasions of individual security?" S. REP. NO. 99-541, at 2.

23. 18 U.S.C. § 2511(1).

24. 18 U.S.C. § 2510(12).

25. *Pharmatrak II*, 329 F.3d at 18 (citing United States v. Steiger, 318 F.3d 1039, 1047 (11th Cir. 2003); Konop v. Hawaiian Airlines, Inc., 302 F.3d 868, 876 (2002)).

26. 18 U.S.C. § 2511(2).

27. 18 U.S.C. § 2511(2)(d).

may permit Web monitors like Pharmatrak to continue intercepting communications through the use of cookies and other devices.

B. Application of Section 2511 Prior to Pharmatrak

¶ 12 Despite the broad scope of the ECPA amendments to section 2511, they have only been used a handful of times to challenge Web-monitoring devices such has cookies. Prior to the First Circuit's ruling in *Pharmatrak II*, each such case held that Web monitoring did not violate even the enhanced prohibitions of the ECPA.

¶ 13 The first of these decisions, *In re DoubleClick*, was a class action brought in 2001 against a company that at the time was the leading online advertising services provider, with over 11,000 clients.[28] DoubleClick acted as an intermediary between companies seeking to advertise online and Web sites willing to sell advertising space on their pages. DoubleClick used cookies to obtain information on visitors to Web sites, information it then used to build personal profiles.[29] The profiles allowed DoubleClick to know who the typical visitors to a particular site were and target the advertisements displayed on that site to their interests. Specifically, when a user with a DoubleClick cookie on his or her hard drive visited a client Web site, the user's computer simultaneously contacted the DoubleClick server, thereby sending personal information and requesting that DoubleClick relay to the Web site advertisements that matched the user's profile.[30] DoubleClick's practices even resulted in an FTC investigation that ultimately found that the company's actions did not violate DoubleClick's own privacy policy.[31]

¶ 14 This finding did not deter a class of Internet users from claiming that DoubleClick violated the Wiretap Act by illegally intercepting their personal information. Although there was no question that DoubleClick had violated the general prohibition against intercepting electronic communications, DoubleClick argued – and the U.S. District Court for the Southern District of New York agreed – that its actions fell within the consent exception. The court found that the client Web sites were "parties to the communications" and that they had consented to the communications being intercepted by DoubleClick.[32] The court then held that DoubleClick's activities were neither criminal nor tortious because this was neither the "primary motivation" nor the "determining factor" in its actions.[33] Instead, the court held that DoubleClick was merely "consciously and purposefully executing a highly-publicized market-financed business model in pursuit of financial gain," an admissible purpose under the consent exception. Interestingly, the consent of the DoubleClick clients was sufficient to satisfy this exception, regardless of whether the users whose personal information was collected actually consented. This is because, according to the court, the ECPA "in no way outlaws

28. *In re* DoubleClick, Inc., Privacy Litig., 154 F. Supp. 2d 497, 500 (S.D.N.Y. 2001).
29. *Id*. at 502-03.
30. *Id*. *See generally id.* at 504 (DoubleClick used the get, post and GIF methods to collect information).
31. *Id*. at 506.
32. *Id*. at 514.
33. *Id*. at 518.

collecting of personally identifiable information or placing of cookies."[34]

¶ 15 Just two weeks later, the U.S. District Court for the Central District of California decided *In re Intuit*, in which a class of visitors to the Quicken.com Web site alleged that the use of cookies violated section 2511.[35] The statement of facts in the case is unusually brief, but it is known that Intuit placed cookies on the plaintiffs' computers. Like DoubleClick, Intuit claimed it was a party to the communications within the meaning of section 2511 and therefore the consent exception should apply.[36] The court agreed, stating that the consent exception should apply because the "[p]laintiffs have failed to state any facts in their complaint which support the allegation that Defendant intercepted electronic communications for the purposes of committing a tortious or criminal act."[37] Therefore, consistent with *DoubleClick*, the court granted Intuit's motion to dismiss, ending the second challenge to Web monitoring brought under section 2511.

¶ 16 Later that same year, two more decisions seemed to signal that such challenges would continue to be dismissed. In *Chance v. Avenue A*, a class action was brought against an online advertising company for conducting activities nearly identical to those of DoubleClick.[38] The U.S. District Court for the Western District of Washington found that the client Web sites had consented to Avenue A's placing cookies on the Web site and intercepting users' communications. "It is implicit in the Web pages' code instructing the user's computer to contact Avenue A … that the Web pages have consented to Avenue A's interception of the communication between them and the individual user."[39] Finally, the court found that there was "no specific evidence … that would reveal a tortious or illegal purpose of the alleged interception."[40] Therefore, the court dismissed the claim under the consent exception to section 2511. Shortly thereafter, in *In re Toys R Us*, the U.S. District Court for the Northern District of California dismissed a claim stating that Coremetrics, a third party hired by Toys R Us, used cookies to "secretly intercept and access Web users' confidential online purchase and Web browsing information, not only at Toys R Us' Web sites, but at other Internet sites."[41] Relying on *DoubleClick* and *Chance*, the court ruled that by employing the services of Coremetrics, Toys R Us had consented to the interception. The court again dismissed the claim, stating that there was no tortious or criminal purpose in these acts, which were intended to assist Toys R Us in profiting from its Web site.[42]

¶ 17 Because of this series of cases, by the end of 2001 it appeared that businesses could use cookies without violating the ECPA amendments to the Wiretap Act. The consent exception to section 2511 had been consistently applied in each case to dismiss

---

34. *Id*. at 510.
35. *In re* Intuit, 138 F. Supp. 2d 1272 (C.D. Cal. 2001).
36. *Id.* at 1278.
37. *Id*.
38. Chance v. Avenue A., Inc., 165 F. Supp. 2d 1153 (W.D. Wash. 2001).
39. *Id*. at 1162.
40. *Id*. at 1163.
41. *In re* Toys R Us, Inc., Privacy Litig., 2001 U.S. Dist. Lexis 16947 at *3 (N.D. Cal. 2001) .
42. *Id.* at *23-28.

claims by users. It seemed that a site using cookies or other Web-monitoring tools could place its activities under this exception by either using the cookies directly or by contracting to do so with a third party. Furthermore, the final element of the consent exception – that the activities not be for a tortious or criminal purpose – would be satisfied if the Web monitor could show that its purpose was to further its business through its Web site. Strikingly, it was never a factor that not only had the users not consented to the interception, but also they were often completely unaware that their personal information was being collected.

III. THE PHARMATRAK DECISIONS

A. Factual Background

¶ 18 Pharmatrak provided Web site operators several services designed to give them statistical information about their visitors. Among these was NETcompare, which Pharmatrak marketed as a package capable of providing comparative data regarding which pages on the client's site were visited by various users.[43] Clients also received information on the traffic of competitors' Web sites if those competitors were also NETcompare subscribers. Among the clients who purchased this service was a group of large pharmaceutical companies that included American Home Products, Pharmacia, SmithKline Beecham, Glaxo Wellcome, and Pfizer.[44]

¶ 19 On each client's site, Pharmatrak installed several lines of code that served to initiate a series of communications between the user's computer, the pharmaceutical client's site, and Pharmatrak's servers. Whenever a user visited a client's site, the code instructed the user's computer to contact Pharmatrak and retrieve a clear GIF.[45] When the user's computer made the request, the Pharmatrak server responded by planting a "persistent cookie" on the user's computer. Persistent cookies do not expire at the end of an online session; rather they are used to collect information about the user's activities and habits over time. A unique identifier associated with each cookie permitted Pharmatrak to record not only where the user traveled on individual client sites, but also whether the same user had visited a competitor's site.[46] On subsequent visits by the same individual to the same client's site, the Pharmatrak server was instructed to retrieve information collected and stored on the user's browser since the cookie had been inserted.[47] The typical user most likely never knew that any of this was taking place.[48]

¶ 20 Pharmatrak collected the information obtained from the NETcompare cookies and organized it into monthly reports to clients. The reports informed clients as to which pages on their site were visited most often, which links were proving to be most popular

43. *Pharmatrak II*, 329 F.3d 9, 13 (1st Cir. 2003).
44. *Pharmatrak I*, 220 F. Supp. 2d 4, 5 (D. Mass. 2002).
45. *Pharmatrak II*, 329 F.3d at 13-14. *See also supra* note 2.
46. *Id.*
47. *Id.* at 14.
48. *Pharmatrak I*, 220 F. Supp. 2d at 8.

among users, and the status of their competitors' traffic.[49] Although Pharmatrak sales materials claimed that the data they collected could be used to create profiles of average users, the actual reports sent to clients consisted merely of percentages of total visitors to the client's site, broken down by location and domain extension. In fact, it was well-documented that Pharmatrak "repeatedly told [clients] that NETcompare … could not collect personal information, and specifically provided that the information it gathered could not be used to identify particular users by name."[50] The reports generally did not contain personally identifiable information about users.[51] In addition, some Pharmatrak clients even obtained explicit assurances from the company, including provisions in the sales contract, that no personally identifiable information would be collected.[52]

¶ 21 Pharmatrack collected individual personal information, however, on a small percentage of users visiting the pharmaceutical companies' sites. This included users' names, addresses, phone numbers, birth dates, genders, occupations, medical conditions, and reasons for visiting the clients' site. The cookies also recorded a small number of e-mail subject lines and sender names. Of the 18.7 million cookies distributed by NETcompare, a sufficient amount of personal information that could be used to generate an individual profile was collected from 232 users.[53] Most of this information collection resulted from user interaction with a particular online rebate form on the Pharmacia site. Because the form utilized the get method, rather than the post method, user-entered personal information was incorporated into the site's URL.[54] When the NETcompare cookies subsequently recorded the URL, this data was also collected. Furthermore, because the cookies often also recorded the immediately preceding URL visited by the user, information posted on non-client sites could be collected.[55] As the First Circuit noted, there was "no evidence that Pharmatrak instructed its clients not to use the get method."[56]

B. The District Court Decision

¶ 22 Several users sued Pharmatrak on behalf of a class of users whose information was collected. Based largely on the analysis of the plaintiffs' expert, who demonstrated that it was possible to develop personalized profiles of 232 individuals using the information on Pharmatrak's servers, the plaintiffs alleged that "Pharmatrak's technology [permitted] defendants to collect extensive, detailed information about plaintiffs and Class members."[57] The plaintiffs claimed these actions violated section 2511's prohibition on the interception of electronic communications.

---

49. *Pharmatrak II*, 329 F.3d at 14.
50. *Id.* at 15.
51. *Id.* at 14.
52. *Id.* at 12.
53. *Id.* at 15, 20.
54. *Id.* at 15-16. *See also supra* note 2.
55. This could occur, for example, if an individual filled out a form on a non-Pharmatrak client's site and then immediately visited a Pharmatrak client's site.
56. *Pharmatrak II*, 329 F.3d at 16.
57. *Pharmatrak I*, 220 F. Supp. 2d at 9.

¶ 23 As with the defendants in the previous cases, Pharmatrak relied on the consent exception. In arguing for summary judgment, Pharmatrak nonetheless conceded that its clients did not directly consent to the collection of personally identifiable information. It instead claimed that "the relevant inquiry is whether the Pharmaceutical Defendants consented to Pharmatrak's NETcompare service."[58] Because each client agreed to have the NETcompare code placed on its sites, Pharmatrak claimed that the consent exception had been met, regardless of what information was actually collected. The plaintiffs argued, however, that the clients must have consented to the personal information being collected in order for Pharmatrak to take advantage of the consent exception.[59]

¶ 24 The U.S. District Court for the District of Massachusetts sided with Pharmatrak, finding that it was irrelevant whether the pharmaceutical clients knew how communications with their site would be intercepted. The mere fact that they consented to the placement of the Web-monitoring device in their code served as sufficient consent.[60] In reaching this decision, the court cited both *DoubleClick* and *Chance*, finding these two cases dispositive in resolving the dispute over Pharmatrak's NETcompare service.[61] As long as the pharmaceutical companies "were parties to communications with Plaintiffs and consented to the monitoring service provided by Defendant Pharmatrak," the consent exception to section 2511 could be invoked to shield Pharmatrak from liability.[62]

C. The Court of Appeals' Reversal

¶ 25 The plaintiffs appealed, again claiming that Pharmatrak violated section 2511 by intercepting electronic communications without the consent of either party.[63] The First Circuit began by noting that the objective of the post-ECPA Wiretap Act is to protect the privacy of communications, adding that the transactions between the plaintiffs and the pharmaceutical Web sites fell within section 2511's broad definition of protected content.[64] The First Circuit then found that the district court had applied an incorrect standard for consent and thus improperly allowed Pharmatrak to rely on the consent exception to section 2511.[65] In so doing, the First Circuit stated that "a reviewing court must inquire into the *dimensions of the consent* and then ascertain whether the interception exceeded those boundaries."[66] The court also noted that while consent may

58. *Id.* at 11.
59. *Id.*
60. *Id.* at 12.
61. *Id.* at 11-12.
62. *Id.* at 12.
63. *Pharmatrak II*, 329 F.3d at 17.
64. *Id.* at 18 (citing Brown v. Waddell, 50 F.3d 285, 289 (4th Cir. 1995); Gelbard v. United States, 408 U.S. 41 (1972)).
65. *Pharmatrak II*, 329 F.3d at 20. This standard was set forth in Griggs-Ryan v. Smith, 904 F.2d 112 (1st Cir. 1990). According to the *Pharmatrak II* court, *Griggs-Ryan* concluded that the consent exception is not merely all or nothing, but rather has fact-specific gradations of consent depending on what the parties have agreed to. *Pharmatrak II*, 329 F.3d at 19.
66. *Pharmatrak II*, 329 F.3d at 19 (emphasis added) (citing Gilday v. Dubois, 124 F.3d 277, 297 (1st Cir. 1997) (quoting *Griggs-Ryan*, 904 F.2d at 119)).

be either express or implied, "it must be actual consent rather than constructive consent."[67] Adhering to a strong burden-of-proof requirement for application of the consent exception, the court added that "consent can only be implied when the surrounding circumstances convincingly show that the party knew about and consented to the interception."[68] Based on this logic, the First Circuit found that the district court failed to inquire as to the precise limits of the pharmaceutical clients' consent.[69]

¶ 26 The First Circuit further reasoned that it would be inconsistent with the principles of the consent exception to hold that the pharmaceutical companies had consented to the specific interceptions Pharmatrak obtained in this case. It therefore held that the clients' consent to have the cookies placed on their sites did not amount to consent to the collection of personal information. In fact, the purchasers of Pharmatrak's NETcompare service specifically requested that no personally identifiable information be collected, and when they learned that personal information had been collected, the clients promptly cancelled the service. The court said holding otherwise "would undercut efforts by one party to require that the privacy interests of those who electronically communicate with it are protected by the other party to the contract."[70] In so doing, the court also rejected the lower court's application of *DoubleClick* and *Chance* to the situation with Pharmatrak. The court noted that in both of those decisions, the Web site operators had purchased a Web-monitoring service "for the precise purpose of creating individual user profiles."[71] It reasoned that those cases were the "mirror image" of *Pharmatrak*, where the clients specifically demanded that no personal information be provided.[72] Finally, the First Circuit found that the users who visited the pharmaceutical Web sites did not consent to Pharmatrak's intercepting their communications, especially where the Web sites gave no notice of Pharmatrak's role. The court noted that "[d]eficient notice will almost always defeat a claim of implied consent."[73] As a result, the consent exception was inapplicable because neither party to the communications had expressed consent to the collection of personal information.

¶ 27 Having ruled that the consent exception did not apply to the collection of personal information, the court addressed another crucial element to a successful claim under section 2511: whether the defendant "intentionally" committed the interception.[74] Because the issue had not been addressed by the district court, the First Circuit remanded the case on this issue. Nonetheless, the court decided to "avoid uncertainty" by delineating the standard for intent under section 2511.[75] It cited the legislative history of

---

67. *Pharmatrak II*, 329 F.3d at 19-20 (citing Williams v. Poulos, 11 F.3d 271, 281-82 (1st Cir. 1993); United States v. Footman, 215 F.3d 145, 155 (1st Cir. 2000)).

68. *Pharmatrak II*, 329 F.3d at 20 (quoting Berry v. Funk, 146 F.3d 1003, 1011 (D.C. Cir. 1998)).

69. *Pharmatrak II*, 329 F.3d at 20.

70. *Id.*

71. *Id.*

72. *Id.*

73. *Id.* at 21 (citing Poulos, 11 F.3d at 281-82; Campiti v. Walonis, 611 F.2d 387, 393-94 (1st Cir. 1979)).

74. *Pharmatrak II*, 329 F.3d at 22. Interestingly, the ECPA amendments changed, from "willfully" to "intentionally," the required mental state a defendant must be shown to have possessed.

75. *Id.* at 23.

the ECPA amendments, which noted that "'[i]ntentional' means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective."[76] In other words, "inadvertent interceptions are not a basis for criminal or civil liability under the ECPA."[77] The court instructed that an act cannot be intentional if it is inadvertent or a mistake. Finally, the First Circuit noted that while an interception is more likely to be deemed intentional if it serves the defendant's self-interest, the merit of the defendant's motive in engaging in the conduct should not be the only consideration.[78]

IV. PHARMATRAK II AND THE PROTECTION OF ONLINE PRIVACY UNDER SECTION 2511

¶ 28 The *Pharmatrak II* decision appears at first to have revived section 2511 as a means of ensuring the privacy rights of Internet users, specifically against the use of Web-monitoring devices. Despite the victory that the First Circuit gave to privacy advocates, however, the decision is significantly limited to its unusual facts. Indeed, the two issues that were central to the court's decision, the consent exception and the intent requirement of section 2511, are likely to limit greatly the statute's applicability to Web monitoring.

A. The Consent Exception

¶ 29 After *Pharmatrak I* was decided, it appeared that online profiling via the use of Web-monitoring devices would continue free from restrictions under section 2511. At the very least, the reversal in *Pharmatrak II* indicates that future cases in the First Circuit must be analyzed using a fact-specific inquiry into the scope of any purported consent. In its ruling, the court sought to prevent a third party from obtaining unlimited consent when the party to the communication clearly had only intended a more limited interception of certain specific communications.

¶ 30 While this reasoning seems sound, it is unlikely to have significant consequences for the use of cookies and other Web-monitoring devices. Overall, the *Pharmatrak II* decision has not done much to change the law as it existed following the *DoubleClick* line of cases. This result is borne out by the key facts of the case. First, unlike the defendants in the earlier cases, Pharmatrak collected information beyond what its clients had requested. This was precisely how the First Circuit distinguished *DoubleClick* and *Chance*. In both of those cases, the clients of the third party purchased Web-monitoring services "for the precise purpose of creating individual user profiles in order to target those users for particular advertisements."[79] The result of the distinction, as stated above, was the court's holding that the consent exception did not apply. Nonetheless, *Pharmatrak II* does not mean that the collection of personal information by using cookies

76. *Id.* (quoting S. REP. NO. 99-541, at 23).
77. *Pharmatrak II*, 329 F.3d at 23
78. *Id.*
79. *Id.* at 20.

is *per se* a violation of section 2511, but merely that a Web-monitoring company cannot claim the consent exception if it collects personal information after stating it would not do so.[80]

¶ 31 Second, the collection of personal information was mostly caused by a specific online form that, when these consequences were revealed, could easily be modified so that no personal information was collected. Furthermore, of the 18.7 million users who had Pharmatrak cookies placed on their hard drives, personal profiles could only be put together for 232 of them. Therefore, the great bulk of individuals using the Web sites were never able to seek relief from the use of the Pharmatrak's cookies. Also, knowing the potential legal consequences of using the get method as delineated in *Pharmatrak II*, businesses that do not wish to collect personal information are likely to avoid it. In that sense, it is likely that companies will learn from *Pharmatrak* and be more cautious in their use of Web-monitoring tools, but this does not mean that the use of such tools will decrease.

¶ 32 The consent exception of section 2511 will continue to give broad liberties to providers that use devices that capture personally identifiable information. So long as consent, even if not from the user, is obtained and not exceeded, the only limitation is that the Web monitor cannot intercept the information "for the purpose of committing any criminal or tortious act."[81] Efforts to collect and package information for business use, as Pharmatrak did with its NETcompare service, have escaped such scrutiny, both in *Pharmatrak* and its predecessors. As a result of these factors, there is little reason to expect that future uses of Web-monitoring tools will fall outside the consent exception.

B. The Intent Element of Section 2511

¶ 33 Another aspect of section 2511 that offers an escape from liability for companies who employ Web-monitoring devices is the requirement that the illegal interception be done "intentionally." The question of whether Pharmatrak "intentionally" intercepted the communications containing personally identifiable information from users was not resolved by the court of appeals in *Pharmatrak II*, but instead remanded to the district court. In its guidance, however, the First Circuit noted that, "[a]s used in the [ECPA], the term 'intentional' is narrower than the dictionary definition of 'intentional.' 'Intentional' means more than that one voluntarily engaged in conduct or caused a result. Such conduct or the causing of the result must have been the person's conscious objective."[82] Thus, the defendant must be found to have acted deliberately and purposefully and the consent cannot have been the product of "inadvertence or mistake."[83]

---

80. The case leaves open the question of whether the consent exception would apply to a situation factually between those of *DoubleClick* and the *Pharmatrak* cases: one in which the party to the communication does not give express consent to the interception of personally identifiable information but does not expressly forbid it, a key factor in *Pharmatrak II*.

81. 18 U.S.C. § 2511(2)(d).

82. *Pharmatrak II*, 329 F.3d at 23 (citing S. REP. NO. 99-541, at 23).

83. *Pharmatrak II*, 329 F.3d at 23

¶ 34 On remand, the district court, acting on the guidance from the First Circuit, found that Pharmatrak had not acted intentionally under the meaning of the ECPA.[84] The court based this decision on three key facts that worked in Pharmatrak's favor. First, while 18.7 million users visited the pharmaceutical companies' Web Sites, Pharmatrak only collected enough information to assemble personal profiles of 232 users.[85] Second, the collection of this personal information was caused by programming errors by third parties, such as errors in Netscape's Navigator browser.[86] Indeed, the facts of this case point to what can rightfully be called a "glitch" that caused a small number of users to have their personal information captured by Pharmatrak's servers — an accidental interaction between computer programs. Finally, Pharmatrak successfully showed that it had no knowledge that the personal information had been collected until the lawsuit was filed.[87] In fact, had Pharmatrak truly wanted to intercept personal information from the Web users, it could have done so far more efficiently than by slowly piecing together information tagged onto the end of URLs.

¶ 35 Nonetheless, as relatively harmless as Pharmatrak's interception of personal information may have been, the case shows the difficulty future plaintiffs will have in satisfying the intent element of section 2511. In a situation where a company collects a small amount of personal information, the company would probably have a reasonable argument that such collection was unintentional. To a certain degree, the statute creates an incentive for companies that engage in Web monitoring, or in any form of data collection for that matter, to maintain a less diligent approach with respect to filtering out personal information. Therefore, the most likely situation where the intent element would be satisfied is one in which the main purpose of the Web-monitoring tool is to collect personal information. Ironically, while this was exactly the case in *DoubleClick* and the other early cases, all the defendants in those cases were able to successfully claim the consent exception.

V. CONCLUSIONS

¶ 36 The interplay between the consent exception and the intent requirement of section 2511 significantly limits its applicability to cookies and other Web-monitoring tools. In fact, there is nothing in section 2511 to prevent Web monitors from collecting information via the use of cookies and other devices *per se*. This became evident in 2001 in *DoubleClick* and the cases that followed it, but the *Pharmatrak II* decision created some uncertainty. Nonetheless, as the discussion above shows, the facts of *Pharmatrak* were relatively unusual, and the First Circuit's finding that the consent exception was not satisfied only applied to a relatively miniscule number of users. The guidance given by the First Circuit shows that it does not believe the great majority of Web monitoring conducted by providers such as Pharmatrak violates section 2511.

---

84. *In re* Pharmatrak, Inc., Privacy Litig., 292 F. Supp. 2d 263 (D. Mass. 2003).
85. *Id.* at 266-67.
86. *Id.* at 267.
87. *Id.* at 268.

¶ 37 Only "rogue" Web monitors, which intentionally intercept personal information without the consent of any party, seem to violate the statute. Therefore, while section 2511 functions to deter the most destructive forms of Internet crime, such as identity theft, the statute does little to protect typical users who are often oblivious to the fact that their every move is susceptible to interception by third parties. In contrast, section 2511 in effect gives safe harbor to legitimate businesses such as DoubleClick, despite the fact that they may not obtain consent from users. This does not mean, however, that users are powerless to prevent their information from being collected. They can fairly easily program their browser to reject cookies, an effective method of preventing private information from being intercepted by third parties. Users can also actively seek out the privacy policy for each Web site before submitting sensitive information. Even then, they should be extremely selective in providing information. Otherwise, a fair argument could be made that, knowing the dangers involved, when users do choose to submit personal information online they are giving a certain degree of consent to its interception.